



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(use as many sheets as necessary)

Sheet 1 of 4

Complete if Known

Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Abdulhakim Nobahar
Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/H.N./	V1	US - 4,202,051	05-06-1980	Davida et al.	
	V2	US - 5,557,346	09-17-1996	Lipner et al.	
	V3	US - 5,623,548	04-22-1997	Aikyama et al.	
	V4	US - 5,625,692	04-29-1997	Herzberg et al.	
	V5	US - 5,625,695	04-29-1997	M'Hraihi et al.	
	V6	US - 5,727,062	03-10-1998	Ritter	
	V7	US - 5,745,577	04-28-1998	Leech	
	V8	US - 5,778,069	07-07-1998	Thomlinson et al.	
	V9	US - 5,870,478	02-09-1999	Kawamura	
	V10	US - 5,982,900	11-09-1999	Ebihara et al.	
	V11	US - 5,998,978	12-07-1999	Connell et al.	
	V12	US - 6,028,454	02-22-2000	Elmasry et al.	
/H.N./	V13	US - 6,345,359	02-05-2002	Bianco	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. ¹	Foreign Patent Number Country Code ³ Number ⁴ Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
/H.N./	V14	JP 09-163469	06-20-1997	ALPHA Corp.	Only Abstract	<input type="checkbox"/>
						<input type="checkbox"/>
						<input type="checkbox"/>

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	07/18/2008
--------------------	----------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Substitute for form 1449B/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Application Number	10/005,105
		Filing Date	December 3, 2001
		First Named Inventor	Paul C. Kocher
		Group Art Unit	2132
		Examiner Name	Abdulhakim Nobahar
Sheet	2	of	4
		Attorney Docket No.	44424162-8721
OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	CiteNo. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/H.N./	V15	VISA INTERNATIONAL SERVICE ASSOCIATION'S PRELIMINARY INVALIDITY CONTENTIONS, FILED IN CASE C04-4143 JW in US District Court for N. District of California, San Jose Division, June 2, 2005.	
	V16	KUHN and ANDERSON, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations." Proceedings of the Second International Workshop on Information Hiding, Portland, Oregon, April 1998, pages 124-142.	
	V17	MENEZES, et al., "CRC Handbook of Applied Cryptography", Boca Raton, Florida: CRC Press LLC, 1996, pages 591-634.	
	V18	VISA INTERNATIONAL SERVICE ASSOCIATION'S FINAL INVALIDITY CONTENTIONS FOR U.S. PATENT NO. 6,278,783 FILED IN CASE C04-4143 JW in US District Court for N. District of California, San Jose Division, June 28, 2007.	
	V19	ALON, et al., "Efficient Dynamic-Resharing 'Verifiable Secret Sharing' Against Mobile Adversary", Mar. 25, 1995.	
	V20	CHARNES, et al., "Comments on Soviet Encryption Algorithm", Springer-Verlag, 1998.	
	V21	MAURER, UELI M., "A Provably-Secure Strongly-Randomized Cipher", Springer-Verlag, 1998.	
	V22	MEIJER and AKI, "Digital Signature Schemes", May 1982, Extended summary of paper presented at CRYPTO 81, Santa Barbara, CA, August 1981.	
	V23	SHAMIR, ADI, "How to Share a Secret", Communications of the ACM November, 1979, Volume 22, Number 11.	
↓	V24	VISA INTERNATIONAL SERVICE ASSOCIATION'S FINAL INVALIDITY CONTENTIONS FOR U.S. PATENT NO. 6,298,442 FILED IN CASE C04-4143 JW in US District Court for N. District of California, San Jose Division, July 16, 2007.	
Examiner Signature	/Abdulhakim Nobahar/		Date Considered 07/16/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Application Number	10/005,105
		Filing Date	December 3, 2001
		First Named Inventor	Paul C. Kocher
		Group Art Unit	2132
		Examiner Name	Abdulhakim Nobahar
Sheet	3	of	4
		Attorney Docket No.	44424162-8721
OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	CiteNo. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/H.N./	V25	BRICKELL, et al., "Fast Exponentiation with Precomputation (Extended Abstract)", Springer-Verlag, 1998.	
	V26	DE ROOIJ, PETER, "Efficient Exponentiation using Precomputation and Vector Addition Chains", Springer-Verlag, 1998, possibly a reprint from Advances in Cryptology, EUROCRYPT '94, 1994.	
	V27	DIMITROV, et al., "An Algorithm for Modular Exponentiation", Information Processing Letters, Volume 66, Issue 3, pp.155-159, May 15, 1998.	
	V28	DIMITROV, et al., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics", IEICE Trans. Fundamentals, Vol. E78-A, No. 1, January 1995.	
	V29	GOLLMAN, et al., "Redundant Integer Representations and Fast Exponentiation", Designs, Codes and Cryptography, 7, 135-151, Kluwer Academic Publishers, Boston, MA, 1996.	
	V30	HONG, et al., "New Modular Multiplication Algorithms for Fast Modular Exponentiation", Springer-Verlag, 1998, from Advances in Cryptology, EUROCRYPT '96, 1996.	
	V31	JEDWAB and MITCHELL, "Minimum Weight Modified Signed-Digit Representations and Fast Exponentiation", Electronics Letters, V. 25, No. 17, Aug. 17, 1989.	
	V32	KOÇ, ÇETIN K., "High-Radix and Bit Recoding Techniques for Modular Exponentiation", Intern. J. Computer Math., v. 40 pp. 139-156, 1991, Gordon and Breach Science Publishers, S.A. (UK).	
↓	V33	EĞECIOĞLU and KOÇ, "Exponentiation using Canonical Recoding," Theoretical Computer Science 129, pp. 407-417, Elsevier, 1994.	
/H.N./	V34	KOÇ, ÇETIN K., "High-Speed RSA Implementation", RSA Laboratories, November 1994.	
Examiner Signature	/Abdulhakim Nobahar/		Date Considered 07/16/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>		Complete if Known	
		Application Number	10/005,105
		Filing Date	December 3, 2001
		First Named Inventor	Paul C. Kocher
		Group Art Unit	2132
		Examiner Name	Abdulhakim Nobahar
Sheet 4	of 4	Attorney Docket No. 44424162-8721	
OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	CiteNo.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/H.N./	V35	LIM and LEE, "More Flexible Exponentiation with Precomputation", Advances in Cryptology, Springer-Verlag, 1998 possibly from CRYPTO '94, August 1994.	
Examiner Signature	/Abdulhakim Nobahar/		Date Considered 07/16/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.